

Security Quickie 20: Confidential Information

Many times a successful information security breach will involve the use or theft of confidential information by nefarious persons. Besides electronic records, paper copies of passwords, management meeting notes, secret business plans, network configuration plans, payment stubs, or the like can also be targeted. An identity thief can also take advantage of such documents, credit card statements, credit offers, and licensing documents to steal company or personal funds.

Unsecured confidential documents can create a serious security risk for your department and the State. Do not leave confidential documents on your desk or lying freely around your workplace when you are not present. Make sure they are placed in a secure location, like a locked drawer or cabinet. Don't leave them at the printer for extended periods of time either, because anybody who wanders by could read or take them.

Often confidential or secret documents are discarded without being destroyed. They can be easily found by illicit "dumpster divers" or even curious co-workers. Make sure you shred confidential documents before throwing them away – it eliminates the possibility that someone else will view them.

